



Product Mode:　DSA-4000/8000 WEB BRAS Series

宽带接入服务器操作手册

Release　Jan 31 2007 type IIII

Table of Contents

1. 总述

D-LINK DSA-4000/8000宽带接入服务器是具有DHCP+WebPortal+Radius功能的接入设备，可以实现给用户动态分配IP地址，让用户通过WEB页面认证后才能上网，而且可以控制用户第一次访问的WEB页面是一个指定的页面（WEB Portal）；同时，用户也可以根据自己的使用习惯选择使用专用的客户端拨号软件进行认证。

根据设备型号的不同，一台D-LINK DSA-4000/8000 可以同时支持1024～8192个用户在线连接。

1.1. 硬件概述：

在D-LINK DSA-4000/8000宽带接入服务器的前端，有相应的网络连接状态以及电源工作情况的指示灯。如图1－1所示设备面板布局：



图1－1 DSA-4000/8000前面板

DSA-4000/8000的型号分为DSA-4000系列和DSA-8000系列。这两个系列设备的主要区别在于其硬件组成和支持同时在线用户数有很大的不同。根据使用的软件版本不同，这两个系列也可以支持PPPoE接入，相应的产品为DSA-4000（PPPoE）和DSA-8000（PPPoE），详细资料请阅读《DSA-4000 PPPoE宽带接入服务器操作手册》。

DSA-4000/8000系列设备前面带有2个固定千兆自适应电口和2个GBIC模块接口（可选配多模、单模、电口模块），其中LAN0(对应命令行enet0)默认为上联口，LAN1～LAN3(分别对应命令行enet1,enet2,enet3)为下联口，Console口用于设备管理和配置。

1.2. 软件概述：

D-LINK DSA-4000/8000宽带接入服务器是一款可以跨三层网络的接入设备，它主要实现以下功能：用户认证（Web和私有客户端）、DHCP（动态IP地址分配）、NAT（网络地址转换）、Radius协议支持、Web Portal功能、Filist报文过滤功能、用户控制、和Radius系统配合完成用户认证、计费等功能。您可以利用Console口或者Telnet方式，方便地对服务器进行配置，使其部分或全部实现上述功能要求。

在初步配置好以后，可以直接通过telnet 登录，进行配置和状态查询。通过与Radius的结合，DSA-4000/8000可以灵活方便的增加用户管理的特性，以及针对不同的环境增加相应的用户策略。DSA-4000/8000还可以实现带宽控制、TCP连接数控制等，在设置用户认证参数时针对不同的服务设定最高带宽限制和TCP连接数控制等。D-LINK DSA-4000/8000的典型应用如图1－4所示：

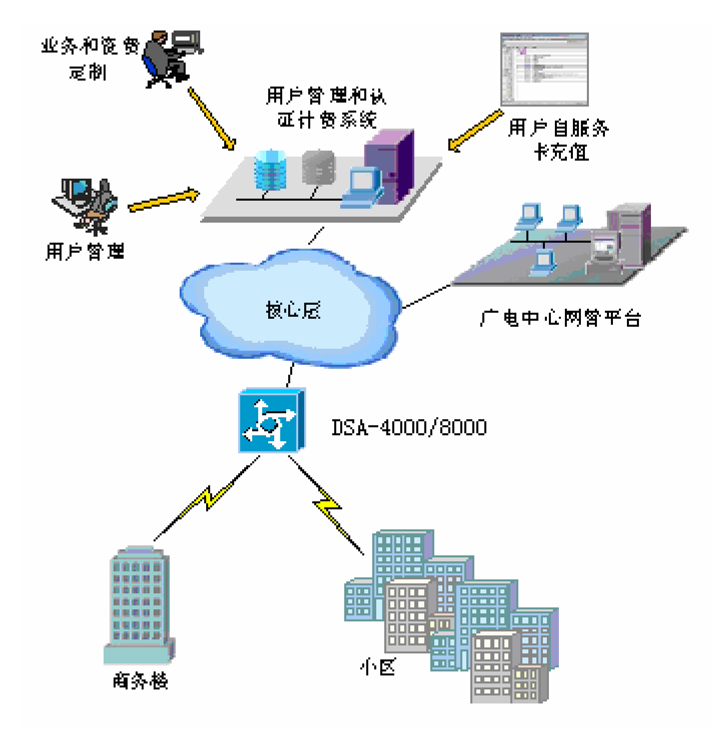


图1－4 D-LINK DSA4000/8000产品的典型应用

2. 硬件描述及安装

DSA-4000/8000采用的Intel 系列处理器为设备提供了强大的处理能力，可最多同时支持8192个用户同时在线。采用19英寸标准机箱能方便地安装上架，可以支持交流电源和直流48V电源。

2.1. 硬件规范：

DSA-4000/8000系列设计紧凑，可靠性高，其硬件规范如下表：

设备型号	DSA-4000/8000
处理器	Intel PIV至强 3.06GHz CPU
内存	1G ECC,128M Flash
外观尺寸	2U 19″标准机箱
网络接口	2个固定100/1000M RJ45电口，2个GBIC插槽（可选配多模、单模、电口模块）
Console	1个DB9串口
重量	12KG
电源	220V AC （43－63Hz） 或者－48V DC （可选配冗余电源）
功耗	300W
工作环境	温度： 0℃－40℃ 湿度： 5％－90％(非凝结)

2.2. 硬件安装:

- 在安装之前，确认电源开关为未打开。
- 机器本身附带有上架设备，按照标准程序把设备固定在机架上。根据设备端口配置情况，用网线或者尾纤连接对应的设备。
- 设备附带有一条串行线，可以通过它与设备的Console 口相连。
- 打开电源，设备启动后可以从Console 口通过超级终端登录进入，设备的硬件运行情况可以从前面的指示灯进行观察。
- 超级终端登录时使用默认的参数：

  速率 9600B/S,数据位8，奇偶校验无，停止位无，流控无。

  登录系统的默认用户名是admin，密码是dlink；进入配置模式（enable模式）的

默认密码是dlink。

注意：为了保证系统的安全，建议设备配置完毕后，一定要修改 enable 模式的密码，密码的设置建议由数字和字母混合组成。

3. 配置 DSA-4000/8000 WEB BRAS 宽带接入服务器

3.1. 基本配置分类：

作为接入设备，每个局点DSA-4000/8000具体的配置应该根据应用环境来设定。DSA-4000/8000的配置可以分为两部分：BRAS自身的配置和与外界进行互连的配置。

3.1.1. 服务器自身的配置：

DSA-4000/8000自身的配置包括端口地址和属性的配置，分别对应命令port和dhcp。port（见port命令详解）对服务器的端口地址进行配置，dhcp（见dhcp命令详解）对端口的属性进行配置。

3.1.2. 与外界互连的配置：

与外界互连的配置内容一般包括Radius配置、NAT（网络地址转换）、认证管理、用户管理、缺省路由、域名服务器等内容。

配置过程应该先配置设备端口属性(见dhcp命令)和允许认证的地址范围（见session命令），与外界互连的配置可以根据需求选择进行。

3.2. 典型配置例子：

下面以一个较为典型的有线电视网络配置来说明应该进行的配置步骤。

3.2.1. 实际环境：

一个有线电视网络，使用cisco7246 CMTS，其下共有1000个左右的Cable Modem用户上网，用户要求访问internet，运营商希望用户上网后第一次访问WEB时打开的页面是http://www.xxxisp.com/；

因CMTS隔断了二层的以太包,PPPoE的接入方式无法使用,只能使用直接面对IP包的DHCP＋Radius的接入。

网管中心给上行端口分配到一个IP地址为192.168.1.2，其上行路由指向地址

192.168.1.1。域名服务器采用公网上的服务器，其地址为202.104.81.245。

计费认证采用Radius方式，Radius服务器的地址为192.168.1.253，加密密钥为“DSA4000”。Radius提供两种服务：local和internet，对应于访问本地和internet的服务类型。

3.2.2. 应用分析：

两幢大楼总共有1000左右的用户，所以采用DSA-4000/8000 1103-III型接入服务器，可以同时支持1024用户上线；

自己分配内部地址，分配在10.1.1.2～10.1.4.254；

自己增加一个管理用户以便进行远程管理；

配置Radius认证计费功能，同时允许管理用户接入上网；

按要求配置路由和域名服务器；

配置两种服务：local和internet；

给服务器命名为HFC-host。

配置Web Portal登录地址是http://www.xxxisp.com/

3.2.3. 配置及分析：

综合上述分析，我们可以抽象出配置命令如下：

1） 有一个DHCP地址池为10.1.1.2～10.1.4.254；

2） 接入服务器有三个端口，一个配置为上行端口其地址为192.168.1.2，一个为接入端口配置地址为10.1.1.1，网管端口可配也可不配；

3） Radius认证计费服务器的地址为192.168.1.253，所用的加密Key为“DSA4000”，同时允许本地认证；

4） 对10.1.1.1～10.1.4.254之间的用户进行地址转换，将该地址段全部采用端口映射到192.168.1.2地址上；

5） 有一本地用户可以进行管理，名字为“manager”，其密码为“aaa”；

6） 缺省的路由的下一跳IP地址为192.168.1.1；

7） 配置域名服务器为202.104.81.245；

8） 提供两种Service，分别为local和internet（需与Radius Server结合起来）；

9） 接入服务器本身的名字为HFC-host。

10）配置Web Portal页面为http://www.xxxisp.com/

针对以上需求，其配置文件内容为(括号内的是注释)：

1) port enet0 ethernet 192.168.1.2 255.255.255.0

（define enet0 address）

2) port enet1 ethernet 10.1.1.1 mask 255.255.252.0

（define enet1 address）

3) dhcp enet1 input

(define enet1 for user access port)

4) dhcp address 10.1.1.2 1000 255.255.252.0 10.1.1.1

（config dhcp server parmater：allow ip from 10.1.1.2 to 10.1.4.254,mask255.255.252.0,default gateway 10.1.1.1）

5) dhcp server enable

6) session address 10.1.1.2 1000

（define legal ip address for access）

7) radius auth ip 192.168.1.253 key DSA4000

（define radius server of authentication）

8) radius auth enable

9) radius acct ip 192.168.1.253 key DSA4000

（define radius server of accounting）

10) radius acct enable

11) user name manager passwd aaa

（define local user and password）

12) local auth enable

13) route add 0.0.0.0 0.0.0.0 192.168.1.1

（config static default route）

14) nat add map enet0 10.1.1.0/22 192.168.1.2/32 portmap

（ config Network Address Translate function）

15) nat add map enet0 10.1.1.0/22 192.168.1.2/32

16) servicename local

17) servicename internet

18) hostname HFC-host

19) nameserver primary 202.104.81.245

20) nameserver secondary 202.104.81.245

21) auth pap

22) Webp url http://www.xxxisp.com/

行号是为方便说明所加

各命令可以解释如下：

1） 1，2 两条命令分别配置上行端口和接入端口的 IP 地址。

2） 第 3 条命令配置 enet1 为认证端口

3） 配置DHCP地址池为10.1.1.2～10.1.4.254的地址段中的1000个地址，该地址段的网关是10.1.1.1。

4） 启用DHCP功能

5） 允许10.1.1.2开始的1000个地址进行接入，即使用户配置固定的IP地址在这一段也可以认证上网

6）－9）配置Radius认证计费服务器的地址为192.168.1.253，加密key为“DSA4000”（**这里使用默认的Radius认证、计费端口1812，1813。如果后台Radius Server使用1645，1646作为认证、计费端口，请配置相应的命令radius auth port 1645,radius acct port 1646**）；

10）增加本地用户，名字为“manager”，密码为“aaa”；

11）配置本地认证，检查本地用户是否符合，如果符合则通过本地认证，否则在Radius服务器上认证；

12）加入缺省静态路由192.168.1.1；

13）-14） 加入NAT规则，把10.1.5.0～10.1.5.255地址段的用户映射到192.168.1.2地址上输出；其中（13）的规则进行端口转换，（14）的规则不进行端口转换，若无（14）规则icmp无法转换ping不出去；

15）16）分别加入local和internet两个服务；

17）配置本机名为HFC-host；

18）19）把primary和secondary域名服务器都指向202.104.81.245；

20）定义认证类型为pap；

21）设置Web Portal页面，用户认证通过后强制登录http://www.xxxisp.com

3.2.4. 补充说明：

上述配置文件的内容可以直接从Console口或Telnet登录进入，手工键入。在配置完成后应该用write命令保存（参见write命令详解）。

用户策略的控制需要与Radius服务器结合起来。其中对用户最高速率的限制是在Radius端设置，通过Radius属性传送到接入服务器实现（参见Radius属性说明）。

对用户服务的控制应该在Radius和DSA-4000/8000同时配置相关的ACL规则。（参见ACL配置命令）

4. 命令详解

在本设备中，命令的操作有两种模式：用户模式和配置模式，分别用>和＃作为命令提示符。用户模式只能查看系统的相关配置，不能进行任何配置操作；配置模式中用户可以实

现各种系统功能的操作。**从用户模式进入配置模式时，先输入enable，再根据提示输入密码；默认的进入配置模式的密码是dlink。**

所有设置的查看都可以用命令加相应的参数（show或list）完成。如果命令没有此类参数，则可以通过show命令后跟相应的命令名参数来实现。

命令语法举例：**port enet**[0/1/2/3] **ethernet** <ip> <mask>

在此命令中port， enet，ethernet为命令关键字，是必须输入的。 []表示必选参数，而/表示多个候选参数中选择一个，<>表示需要输入的参数。

命令行系统支持上下键来调用历史命令,用户可以利用上下键调用此前用过的10个历史命令。同时可以利用Backspace键对命令进行修改，这些编辑功能对命令的输入十分方便。

在本设备中，IP地址和掩码一般用4位点分十进制数表示，而掩码有时也用10进制数表示。

各命令具体的解释入下：

4.1. ？

【用法】：?

【作用】：显示可用命令。

【例如】:

- DSA4000> ?

```
show          show system information
ping          test network
enable        get full right
```

显示当前命令模式下的可用命令。

4.2. acl

【用法】: acl 0/1/2/3/4/5/6/7 block/pass/only

acl 0/1/2/3/4/5/6/7 enable/disable/show

【作用】:第一条命令定义指定编号的 acl 规则的行为是阻止（block)、放行（pass)、只允许（only)。acl 规则是用来开展服务定制的(该功能必须和 Radius server 相配合)，它定义了一组 IP 地址和该 acl 规则的行为。当用户进行认证时，选择了相应的 servicename，

那么该用户就只能根据相关联的 acl 规则进行访问。acl 规则的定义见 aclcfg 命令的相关解释。

第二条命令指定相应的 acl 规则是否开启和查看 acl 设置。

【例如】:

- DSA4000 # acl 0 block
- DSA4000 # acl 0 enable
- DSA4000 # acl 0 show

  The ACL 0 List

  Service:DSA4000

  network address   network netmask

  192.168.1.0   255.255.255.0

  该命令显示了 acl 0 设定的 IP 地址范围是 192.168.1.0，该规则和 service DSA4000 相关联。当用户认证时选择的 service 是 DSA4000 时，该用户不能访问 192.168.1.0 子网，但是可以访问其他子网。

【相关命令】:

- aclcfg 0/1/2/3/4/5/6/7 get/put tftp_server filename

4.3. aclcfg

【用法】: aclcfg 0/1/2/3/4/5/6/7 get/put tftp_server filename

【作用】: 下载或者上传 acl 配置文件。

【例如】:

- DSA4000 # aclcfg 0 get 192.168.0.168 acl0.txt

  将 acl0 规则的配置文件 acl0.txt 从 TFTP Server 192.168.0.168 下载到 BRAS。

- DSA4000 # aclcfg 0 put 192.168.0.168 acl0.txt

  将 acl0 规则的配置文件从 BRAS 上传到 TFTP Server 192.168.0.168 并命名为 acl0.tx。

【相关命令】:

- acl 0/1/2/3/4/5/6/7 enable/disable/show
- acl 0/1/2/3/4/5/6/7 block/pass/only

【注意事项】:

1、 aclcfg 文件的必须是 txt 文件，命名以能够表明 acl 相关内容为原则。

2、 aclcfg 文件的格式为：

vod

192.168.2.0 255.255.255.0

其中 vod 为 servicename,192.168.2.0 255.255.255.0 是 vod 服务对应的 IP 地址。

3、如果多次上传 aclcfg 文件，在上传前先执行 acl 0/1/2/3/4/5/6/7 disable 命令，上传完文件后再执行 enable 命令，使新的 acl 规则生效。

4.4. arp

【用法】: arp bind <ip> <mac>

arp bind show

arp del <ip>

【作用】: 绑定、显示、删除 ARP 表项。

【例如】:

- DSA4000 # arp bind 192.168.0.1 00:01:02:97:89:25

  将 192.168.0.1 和它的 MAC 地址 00:01:02:97:89:25 绑定，使其成为静态 ARP 表项。这个命令主要目的是为了防止设备对接时因为 ARP 协议配合不好而导致通信中断的情况发生，用户可以根据现场具体情况进行配置。

- DSA4000 #arp bind show

  ARP BIND TABLE

  192.168.0.1 00:01:02:97:89:25

  显示已经绑定的

- DSA4000# arp del 192.168.0.1

  删除绑定的 ARP 表项。

4.5. auth

【用法】：auth chap/pap

【作用】：定义用户进行Radius认证时的认证类型。

【例如】：

- DSA4000 # auth pap

  定义BRAS用户进行Radius认证时的认证类型为PAP（Password Authentication Protocol）。

- DSA4000 # auth chap

  定义BRAS用户进行Radius认证时认证类型CHAP（Challage Handshake Authentication Protocol）。

4.6. backup

【用法】：backup

【作用】：备份系统当前IOS软件，当系统升级或者启动失败时可以使用备份的IOS软件进行启动或者工作。

【例如】:

- DSA4000 # backup

  将系统当前的IOS软件备份到内存中。

如果系统启动异常时，可以在启动时选择b，利用备份的IOS进行启动。下面是启动过程的抓屏文件：

```
Press any key to stop auto-boot...
 4
DSA4000> ?
c               - run ios
b               - run backup ios
n               -run from network
DSA4000>b
Mount Hard Disk... done.
Loading IOS... 4887744
Starting at 0x308000...
```

所有设备在出厂前都对当前使用的IOS版本文件进行了备份，当您升级新的版本文件并

再次执行backup命令时会用最新的IOS作为备份版本文件，该文件保留在系统内置的Flash卡中。

4.7. back_rt

【用法】：

back_rt　enable|disable

back_rt　set default　<weight>

back_rt　set <gw>　<weight>

back_rt　del <gw>

【作用】：有两个上行出口时配置每个出口的负载比例，用于双出口负载分担。

【例如】：

- DSA4000 # back_rt enable

  激活双出口路由负载分担功能

- DSA4000 #back_rt set default 6

  设置默认路由的负载为整个出口流量的60%

- DSA4000 #back_rt set 192.168.1.2 4

  设置另外一个出口 192.168.1.2 的下一跳负载整个出口流量的 40%

- DSA4000 #back_rt del 192.168.1.2

  删除另外一个出口的配置。

【注意】：因为目前的 D-LINK DSA-4000/8000 版本中的 ACL，TCPlimit，流量计费等功能和 enet0 相关联，所以当采用双出口负载分担时第二出口的上述功能不能够正常工作，因此只有不使用上述功能时才可以使用该功能。负载分担的比例一般为 M:N，M 和 N 均小于 10。

4.8. cfg

【用法】：cfg put|get tftp_server　filename

cfg restore

【作用】：从tftp服务器获取或保存配置文件，一般情况下建议从上行接口上传或者下载配置文件。这样能够避免有时配置下行接口为认证口时，而用户没有认证而进行配置文件的上传或者下载导致的失败行为。

【例如】:

- DSA4000 #cfg get 192.168.1.2 config.txt

  从tftp服务器（地址为192.168.1.2）中获取名字为config.txt的文件作为自己的配置文件。

注意：如果要使config.txt文件生效，你可以在下载完成该文件直接执行reboot命令，使系统重新启动后调用新的config.txt配置文件，不要去执行write命令，否则还会把当前使用的配置文件作为启动配置文件来调用。

- DSA4000 #cfg put 192.168.1.2 config.txt

  把当前系统的配置文件上传到地址为192.168.1.2的tftp服务器上，并命名为config.txt。

- DSA4000 #cfg restore

  将配置文件恢复成出厂默认配置，出厂默认配置是对任何参数都不予以配置（除了系统默认的参数）。

4.9. dhcp

【用法】 dhcp address <begin_ip> <num> <mask> <route>

dhcp umac enable/disable

dhcp umac list

dhcp umac get|put tftp_server filename

dhcp relay <ip> <network>

dhcp enet[1/2/3] input

dhcp lease <minute>

dhcp server enable|disable

dhcp agent <server_ip> <inport>

【作用】：配置 DHCP 相关参数

- dhcp address <begin_ip> <num> <mask> <route>

  当 DSA-4000/8000 作为 DHCP Server 时，配置 DHCP 地址池中分配给用户的 IP 地址、掩码、网关等参数。

- dhcp umac enable/disable

是否开启 IP 和 MAC 绑定功能。如果开启，则该 MAC 的用户只能分配指定的 IP 地址使用。

- dhcp umac list

  显示绑定的 IP 和 MAC 地址列表。

- dhcp umac get|put tftp_server filename

  下载或者上传用户 IP 和 MAC 绑定关系文件。

- dhcp relay <ip> <network>

  当 DSA-4000/8000 启用 DHCP Relay 功能时，配置 DSA-4000/8000 中继的 DHCP 子网。

- dhcp enet[1/2/3] input

  设置端口的属性，如果设置端口为 input 属性，则该端口作为用户接入端口(此时该端口连接的用户必须进行认证才可以上网)，否则可以作为普通路由端口。当启用 DHCP Server 功能时，该端口的用户可以通过 DHCP 分配地址。

- dhcp lease <minute>

  设置 DHCP 协议分配 IP 地址的租期。

- dhcp server enable|disable

  开启或者关闭 DSA-4000/8000 的 DHCP Server 功能。

- dhcp agent <server_ip> <inport>

  当 DSA-4000/8000 作为 DHCP Agent 功能使用时，指定 DHCP Server 的地址和请求 DHCP 地址分配的下行端口。一般指定端口 1 为 DHCP 分配地址的下行口，配置此命令前必须先给端口 1 配置接口地址。

【例如】：

- DSA4000 # dhcp address 10.1.1.2 253 255.255.255.0 10.1.1.1

  当 DSA-4000/8000 作为 DHCP Server 时，分配 10.1.1.2 开始的 253 个地址给用户，该子网的掩码是 255.255.255.0，用户网关地址为 10.1.1.1。

- DSA4000 #dhcp umac enable

  激活 IP 和 MAC 绑定功能。

- DSA4000 #dhcp umac list

  显示 IP 和 MAC 绑定表的内容。

- DSA4000 #dhcp umac get 192.168.0.189 umac.txt

  从 192.168.0.189 的 TFTP Server 下载用户 IP 和 MAC 绑定关系的文件 umac.txt。其

中当使用 put 命令时，上传当前用户的 IP 和 MAC 地址绑定关系文件到 TFTP Server 指定的目录下并命名为 umac.txt。

- DSA4000 #dhcp relay 192.168.1.1 192.168.1.0

中继网关为 192.168.1.1，子网为 192.168.1.0 的用户发送的 DHCP 请求报文。

- DSA4000 #dhcp enet1 input

设置 enet1 口为用户接入端口，该端口连接的用户可使用 DHCP 协议进行地址分配，同时该端口连接的用户也必须进行认证才可以访问外网。

- DSA4000 #dhcp lease 600

设置 DHCP 分配的 IP 地址租期为 600 分钟。

- dhcp server enable

DSA-4000/8000 启用 DHCP Server 功能。

- DSA4000 #dhcp agent 192.168.0.100 1

当 DSA-4000/8000 作为 DHCP agent 设备时，此时进行地址分配的 DHCP Server 的地址为 192.168.0.100，由端口 1 的用户发起 dhcp 请求。

【注意事项】:

A、当配置 DSA-4000/8000 为 DHCP Relay 功能或者 DHCP Agent 功能时，必须执行 dhcp server disable 命令。

B、目前的版本只支持一个端口作为 dhcp agent，暂不支持多端口作为 dhcp agent。

C、当 DSA-4000/8000 工作在桥接模式下时，目前系统不能作为 DHCP Server 进行地址分配。

当启用 dhcp mac 绑定功能时，该配置文件必须是 txt 格式，IP 和 MAC 的对应格式如下：

0000e8e04412 192.168.2.3 255.255.255.0 192.168.2.1

用户 MAC　　用户 IP　　IP 掩码　　用户网关

其中用户 MAC 的表示必须以小写字母和数字组成，在整个脚本的最后必须以回车符结束。

特别注意的是您配置的脚本中的地址不能和 dhcp address 命令配置的地址范围相重合，否则程序会打印报错信息。

【相关命令】:

session address ip <num> [pass|pass_out]

4.10. debug

【用法】：debug lcp/ipcp/radius on/off

debug nat

debug show

【作用】：配置调试开关

【例如】:

- DSA4000# debug radius on

  打开RADIUS 调试开关。

- DSA4000#debug show

  显示各调试开关的设置。

- DSA4000#debug nat

  显示NAT资源的使用情况。

【注意事项】：

该命令中的lcp/ipcp用于PPPoE的debug信息，DSA-4000/8000没有用。

debug开关主要用于技术人员判断系统故障时使用，平时应该处于off状态。

4.11. enable

【用法】：enable

【作用】：从普通模式进入到配置模式，需要输入使能的密码。

【例如】:

- DSA4000> enable

  进入配置模式。

- DSA4000# enable passwd

  修改enable的密码，需要输入2次确认。

【注意】:为了保证系统的安全，建议用户修改默认的enable密码。Enable密码修改后，无论是telnet登陆还是console口管理，都必须使用使用修改后的密码进行登陆。

4.12. exit

【用法】：exit

【作用】：退出配置和监控。

【例如】：

- DSA4000# exit

  DSA4000>

  退出配置模式。

4.13. filist

【用法】：filist add/del port block/pass in/out protocol src [srcport scmp port]

dst [dstport dcmp port] [quick]

filist flush/list

src_ip_pool 和map_ip_pool格式为ip/prefix，其中ip为ip地址段，prefix为地址中网络部分所占位数（十进制表示的掩码位数）。

【作用】：设置、清除或者显示报文过滤信息，该功能类似Cisco公司的ACL命令。

【参数说明】：

add/del　增加/删除

port　端口(例如enet0， enet1等）

block/pass　阻塞/通过

in/out　进入/输出（针对端口而言）

protocol　针对的协议(icmp/udp/tcp)

src　源地址(地址/掩码)

srcport scmp port　（可选）源端口

格式：srcport (‘>’ ‘<’ ‘>=’ ’ ’<=’ ‘=’) portnum

其中srcport是关键字，scmp是以上的比较符号， portnum是数字；

dst　目的地址(地址/掩码)；

dstport dcmp port　（可选）目的端口，

格式：dstport (‘>’ ‘<’ ‘>=’ ’ ’<=’ ‘=’) portnum，

其中dstport是固定字，dcmp是以上的比较符号， portnum是数字；

quick　(可选)找到规则后就直接返回，不再往下进行匹配。

【例如】：

- DSA4000#filist flush

  清除所有filist规则。

- DSA4000# filist list

  显示所有filter规则。

- DSA4000# filist add enet0 block out tcp 10.1.1.0/24 srcport > 1024 192.168.1.168/32 dstport = 23 quick

  在端口enet0上针对出去的tcp数据设置过滤规则，阻塞 源地址在10.1.1.1 ～ 10.1.1.255网段、源端口大于1024，目的地址为192.168.1.168、目的端口为23的数据包。在匹配该规则后，不再往下匹配。

- DSA4000#filist add enet0 pass out tcp 0.0.0.0/0 0.0.0.0/0

  在端口enet0针对出去的tcp数据设置过滤规则，让所有的数据通过。

- DSA4000#filist add enet0 pass out udp 0.0.0.0/0 0.0.0.0/0

  在端口enet0针对出去的udp数据设置过滤规则，让所有的数据通过。

- DSA4000# filist add enet0 pass out icmp 0.0.0.0/0 0.0.0.0/0

  在端口enet0针对出去的icmp数据设置过去规则，让所有的数据通过。

【注意】：为了保证系统的安全，建议在现场调试时block掉135，137，138，139，445，554，icmp等端口和协议，防止病毒报文的传播。

4.14. ha

【用法】：ha enable|disable

ha timeout <second>

ha chk_interval <second>

ha set mon <ip> <rt>

ha del mon <ip>

【作用】：配置两台 DSA-4000/8000 的高可用性相关参数，一般情况下 DSA-4000/8000 产品架设在网络的出口。为了防止意外情况发生，有可能使用 2 台设备连接在网络出口，其中一台设备只作为备用机使用，监控主用设备的状态：当主用设备死机或者电源故障时，由备用设备接管主用设备进行工作。**详见相关专题文档的详细描述。**

- DSA4000＃ha enable|disable

ha 功能打开或者关闭

- DSA4000＃ha timeout <second>

  配置多长时间认为监控 ip 地址不合法

- ha chk_interval <second>

  配置多处时间检查一次监控的 ha 地址是否正常工作。

- ha set mon <ip> <rt>

  配置需要监控的地址和对应路由器地址，如果发现监控地址没有 alive, 修改对应端口地址为监控地址。

- ha del mon <ip>

  删除 HA 的监控地址

【例如】:

DSA4000＃ha enable

打开 ha 功能。

DSA4000＃ha set mon 192.168.1.2 192.168.1.1

配置监控的 BRAS 的地址为 192.168.1.2,同时监控其相连的路由器接口 192.168.1.1 是否处于 alive 状态。

【相关命令】: show ha_info

4.15. hostname

【用法】：hostname <name>

【作用】：配置主机名。

【例如】:

- DSA4000# hostname bras

  bras#

  定义主机名为 bras。

4.16. icmpin

【用法】: icmpin enable/disable/show

【作用】: 是否允许 icmp 协议使用。

【例如】：

- DSA4000#icmpin enable

  允许使用 icmp 协议，可以利用 ping 命令进行测试。系统默认情况下该功能是关闭的。

【注意】：为了防止黑客攻击系统或者冲击波病毒的危害，平时请将 icmpin 功能关闭，当检查网络故障时可以短时间打开 icmpin 功能。

4.17. local

【用法】: local auth enable/disable

【作用】：配置是否进行本地认证，可以和Radius结合形成完整的认证系统。如果只有Radius认证没有设置本地认证，则BRAS的管理用户不能Telnet登录设备。本地认证通常用来判断Radius认证的故障，这样能够简化网络故障的判断。

【例如】:

- DSA4000# local auth enable

  允许本地认证。

- DSA4000# local auth disable

  禁止本地认证。

【参考命令】：radius，user。

4.18. logger

【用法】：looger on ip port

logger off

logger url on/off

【作用】:打开或者关闭系统的上网日志功能。

【例如】：

- DSA4000#logger on 192.168.0.123 12000

  设置上网日志接收服务器为 192.168.0.123，接收端口为 12000。

- DSA4000#logger off

  关闭系统上网日志功能。

- DSA4000＃logger url on

日志发送记录信息中包括 url 信息，如果是 off 状态，用户上网日志中只包括源 IP、目的 IP、源端口、目的端口、协议、上网时间等记录。

【注意】：上网日志功能是用来对用户的上网行为进行记录和分析的模块，该日志信息的接收和分析必须安装 DSA-4000/8000 专用的日志接收和分析软件。

因为上网日志记录中上网时间是以 DSA-4000/8000 的系统时间为准，所以在调试时一定要通过 time 命令校正系统时间，并保存配置重启设备，以便设置的时间能够生效。

由于上网日志记录的信息量很庞大，因此建议如果用户使用日志功能时，尽量使用单独设备作为日志采集设备，避免设备负担过重。

4.19. multi

【用法】：multi on/off

multi proxy ip port

multi show

【作用】：组播路由功能配置。

【例如】：

- DSA4000# multi on

  开启组播功能。

- DSA4000#multi proxy 224.1.1.1 23322

  配置 DSA-4000/8000 为组播组 224.1.1.1 的代理，端口号为 23322。

- DSA4000# multi show

  multi on

  multi proxy 224.1.1.2 23322

  显示组播配置的结果。

【注意】:

D-Link 的 DSA-4000/8000 实现了 DVMRP 或者 IGMP 功能，暂不支持 PIM-SM 和 PIM-DM,因为 DVMRP 组播协议使用较少，所以只提供了组播代理功能。目前 D-Link 的 BRAS 版本只支持一个组播流，暂不能支持多个组播源

4.20. nameserver

【用法】：nameserver primary/secondary <ip>

【作用】：配置DNS服务器。

【例如】:

- DSA4000#nameserver primary 192.168.1.2

  把第一域名服务器指向地址192.168.1.2

- DSA4000# nameserver secondary 192.168.1.88

  把第二域名服务器指向地址192.168.1.88

【注意】:DNS Server的配置只有在用DHCP分配网络参数时有用。

4.21. nat

【用法】：nat add/del map/rdr <port> <src_ip_pool> [srcport port] <map_ip_pool> [dstport port] [portmap]

nat list/flush

src_ip_pool 和map_ip_pool格式为ip/prefix，其中ip为子网地址，prefix为地址中网络部分所占位数（即10进制表示的掩码长度）。

【作用】：配置地址转换表。该命令应该设置port参数之后进行设置。一般地，<port>参数是网络端口号（如enet0），src_ip_pool是某个地址池中的一段地址。

map是对源地址进行映射，改变数据包的源地址，对数据的目的地址不做任何改变,就是常说的动态NAT。

rdr是对目的地址进行改变，重新定向数据的目的地址，对数据的源地址不做任何改变（有的也称静态NAT，或者反向NAT）。

【注意】：**使用rdr规则时，重定向的地址只能是一个，因此掩码都应该是32。并且src_ip_pool地址应该是外部地址，<map_ip_pool>为内部地址。**

【参数说明】：

add/del　　增加/删除

map/rdr　　映射/重定向

port　　　　端口

src_ip_pool 源ip地址(ip/mask)

srcport port （用于rdr规则，指定目的地址的端口，可选）

map_ip_pool 目的ip地址(ip/mask)

dstport port （用于rdr规则，指定转向后的端口， 可选）

portmap （用于map规则，可选）

【例如】:

- DSA4000# nat add map enet0 10.1.1.0/24 202.96.196.32/30

  在绑定了端口名字为enet0的上行接口上，将地址为10.1.1.0到10.1.1.255的地址转换为202.96.196.32到202.96.196.35的一段地址上。

- DSA4000# nat add rdr enet0 10.1.1.2/32 192.168.1.2/32

  在enet0端口上，把所有访问10.1.1.2的数据重定向到192.168.1.2上去。

- DSA4000# nat add rdr enet0 10.1.1.2/32 srcport 23 192.168.1.2/32 dstport 23

  在enet0端口上，把所有到10.1.1.2的23端口的数据重定向到192.168.1.2的23端口上。

- DSA4000#nat add map enet0 10.1.1.0/24 202.96.196.3/32 portmap

  在绑定了端口名字为enet0的接口上, 将地址为10.1.1.0 到 10.1.1.255 的地址转换到地址202.96.196.3上去，并在此地址上进行端口转换。

- DSA4000# nat del map enet0 10.1.1.0/24 202.96.196.32/30

  删除名字为“enet0的端口上，将地址为10.1.1.0到10.1.1.255的地址转换为202.96.196.32到202.96.196.35的一段地址”这样一条规则。

- DSA4000# nat list

  显示所有nat有效规则。

- DSA4000# nat flush

  删除所有nat规则和连接。

4.22. no

【用法】：no user/servicename/snmp name

no port enet[0/1/2/3] vlan_id <num>

no dhcp address ip num

no dhcp agent

no dhcp relay ip net

no dhcp enet[1/2/3] input

no session address ip num

no session ip

【作用】：

- no user/servicename/snmp name

  删除本地用户认证用户，删除配置的服务名，删除SNMP community的参数。

- no port enet[0/1/2/3] vlan_id <num>

  去掉端口接收的指定VLAN tag配置。

- no dhcp address ip num

  删除DHCP分配的指定地址段。

- no dhcp agent

  删除指定的dhcp server。

- no dhcp relay ip net

  删除dhcp relay指定的子网。

- no dhcp enet[1/2/3] input

  取消端口的接入端口属性。

- no session address ip num

  删除设置的允许接入的地址范围。

- no session ip

  强制指定IP地址的用户下线

【例如】:

- DSA4000# no user admin

  删除用户名为admin的本地用户。

- DSA4000# no servicename serv1

  删除名字为serv1的服务。

- DSA4000#no snmp DSA4000

  删除名字为DSA4000的snmp community。

- DSA4000#no session 10.1.2.23

  强制在线用户10.1.2.23下线。

【参考命令】user，servicename，snmp，session，dhcp,port。

4.23. ping

【用法】：ping <ip>

【作用】：检测目标地址的连通性。在运行本命令之前，必须先配置好设备的接口地址或者地址池，并且要检查filist中是否禁用了icmp协议，同时检查icmpin命令是否允许icmp功能使用。

【例如】：

- DSA4000# ping 202.96.196.5

检测目标地址为202.96.196.5的连通性。

【参考命令】：port，filist，icmpin。

4.24. port

【用法】：port enet[0/1/2/3] ethernet <ip> <mask>

port enet[0/1/2/3] vlan_id <num>

port enet[0/1/2/3] force <speed> <full/half>

port enet[0/1/2/3] auto

port enet0 swap enet[1/2/3]

port enet[0/1/2/3] bridge enet[0/1/2/3]

port nobridge

port bridge_out <ip>

port nobridge_out <ip>

port enet[0/1/2/3] fc on/off

port show

【作用】：配置通信端口封装类型和地址，以及VLAN配置、桥模式工作方式的配置，应该在配置过程的前期就使用此命令进行相关配置。如果改变了原来的端口配置，需要保存配置并重新启动接入服务器。

【例如】：

- DSA4000# port enet0 ethernet 192.168.1.10 255.255.255.0

把端口0配置（一般作为上行端口）为以太封装类型，ip地址为192.168.1.10，掩码为255.255.255.0。

- DSA4000#port enet1 vlan_id 2

  配置端口enet1接收vlan tag为2的报文。

- DSA4000# port enet2 force 100 full

  配置端口enet2强制为100M，全双工工作方式。

- DSA4000# port enet2 auto

  配置端口enet2为自动协商工作方式。

【注意事项】：

关于端口工作模式的设置，一般情况下必须设置成auto模式，由双方设备自动协商速率和双工模式。因为受网络控制芯片设计的限制，不同厂家的网络设备对接时可能出现端口工作模式不一致的情况，一般的处理方式有：

A、 配置好端口工作模式后（如 auto 或者一方强制工作模式），保存配置后重启双方设备或者重新插拔一下网线，触发设备端口工作模式协商过程。

B、 强行配置双方端口的工作模式保持一致，如都强制为 100M Full；并保存配置后重启设备进行重新连接。因为有些网络芯片当一方为 auto，另一方设置为 100M full 时可能的结果为 100M half 和 100M full，如 Cisco 公司的设备，所以双方必须强制相同的工作模式。

C、 光口工作模式不能强制，只能是 auto（实际上只有 1000M full 一种模式）。

- DSA4000# port enet1 fc on

  配置端口1打开流控开关，默认情况下所有端口流控都是关闭的。

- DSA4000# port enet0 swap enet2

  将上联端口由enet0交换到enet2，这个命令主要是为了在组网中灵活调整上行接口类型。因为DSA-4000/8000 中enet0,enet1为光口时，默认enet0为上行接口。当网络中使用的上联端口为电口时，需要配置命令将默认的上行端口enet0交换到enet2，此时enet0的物理连接变换到了enet2，但是NAT，filist、接口地址等配置仍旧和enet0的配置相关联。

- DSA4000# port enet0 swap enet0

  取消端口交换功能，enet0恢复作为上联端口。

- DSA4000# port enet3 bridge enet0

配置系统中enet3的端口报文桥接到enet0,这是桥接模式专用命令。

- DSA4000#port nobridge

  取消系统的桥接工作模式，这是桥接模式专用命令。

- DSA4000# port bridge_out 192.168.0.2

  设置系统桥接工作模式时将报文传送到192.168.0.2，这是桥接模式专用命令。

注意：桥接模式下和DSA-4000/8000 enet0接口相连的同一子网的设备要和DSA-4000/8000进行通信，必须配置此命令。该命令可以配置多条。

- DSA4000# port nobridge_out 192.168.0.2

  删除系统桥接模式时将报文传送到192.168.0.2的设置，桥接模式专用命令。

- DSA4000#port show

  检查端口配置。

【参考命令】：reboot。

【注意事项】：

桥接模式是针对复杂网络要求DSA-4000/8000采用透明工作方式而设计的，它的典型应用环境是当DSA-4000/8000处于核心交换机和防火墙设备中间时,此时要求DSA-4000/8000透明接入网络。

假设核心交换机的上行接口地址为192.168.250.1/24,防火墙的下行接口地址为192.168.250.2/24,此时DSA-4000/8000工作在桥接模式下,它的enet3端口连接核心交换机，enet0端口连接防火墙。

此时DSA-4000/8000的配置如下：

- DSA4000# port enet3 input
- DSA4000# port enet3 ethernet 192.168.250.3 255.255.255.0
- DSA4000# port enet3 bridge enet0（端口 3 桥接到端口 1）
- DSA4000# port bridge_out 192.168.250.2

  （桥接模式的下一跳输出到192.168.250.2）

此时系统的nat,filist,radius，route等和普通路由模式的配置相同。

【注意】：截至该手册本地修订时，桥接工作模式只是在DSA-4000/8000 系列产品中提供，DSA-4000/8000 1103系列产品没有提供桥接工作模式。

桥接工作模下，当Radius Server连接在3层交换机以下时，需要配置到Radius Server的回指路由；其它情况下可以不用配置静态路由，包括默认路由和回指路由。

4.25. proxyarp

【用法】：proxyarp add/del <ip> <mask>

proxyarp show

【作用】:代理一段IP地址的ARP应答。当DSA-4000/8000的IP Pool或者NAT的目标映射IP Pool是从本地Subnet（与上行以太网端口处于同一Subnet）再分配出来,而不是独立可路由的subnet时，此时配合 nat 命令而设置相应的proxyarp。

【例如】:

本地管理网段为202.104.87.1, mask为255.255.255.240。考虑用户的IP为192.168.1.0/24，且把202.104.87.1和202.104.87.2 两个IP地址用于NAT目标IP Pool。此时的设置应该为：

- DSA4000#nat add map enet0 192.168.1.0/24 202.104.87.1/30 portmap(TCP,UDP 的端口映射)；
- DSA4000#nat add map enet0 192.168.1.0/24 202.104.87.1/30 (非TCP,UDP的NAT，可选)；
- DSA4000# proxyarp add 202.104.87.1 255.255.255.252

最后一条命令设置DSA-4000/8000接入服务器代理202.104.87.1- 2两个IP地址的ARP应答。

4.26. radius

【用法】: radius [b]auth/[b]acct/dupacct ip <ip> key <key>

radius [b]auth/[b]acct/dupacct retry <num>

radius [b]auth/[b]acct/dupacct timeout <seconds>

radius [b]auth/[b]acct/dupacct port <port>

radius [b]auth/[b]acct/dupacct enable/disable

radius auth_switch_num <num>

radius acct_switch_num <num>

radius mon_primary on/off

radius mon_down on/off

radius mon_down_num <num>

radius mon_interval <seconds>

radius show

【作用】：配置远程拨入用户认证服务器和计费服务器相关参数和Radius主备切换功能。其中，bauth是备份认证服务器、bacct是备份计费服务器、dupacct是对帐服务器。

【例如】：

- DSA4000#radius auth enable

  采用radius认证。

- DSA4000#radius auth ip 202.96.196.2 key DSA4000

  配置认证服务器IP 地址为202.96.196.2, 通信密钥为DSA4000。

- DSA4000#radius acct ip 202.96.196.2 key DSA4000

  配置计费服务器IP 地址为202.96.196.2, 通信密钥为DSA4000。

- DSA4000# radius auth timeout 10

  认证请求如10秒没收到应答, 将重发该报文，系统默认的时间为5秒。

- DSA4000# radius auth retry 5

  当认证报文没有收到Radius Server的响应报文时，DSA-4000/8000 重新发送的认证报文的次数，系统默认的重发次数是3次。

- DSA4000# radius auth port 1812

  配置认证服务的认证端口为1812。

- DSA4000# radius dupacct ip key DSA4000

  配置对帐服务器的地址为202.96.196.2 ，通信密钥为DSA4000。

【注意事项】

当配置radius认证时，需要配置认证、计费服务器的地址、通信密钥、端口号，并且要打开 DSA-4000/8000的认证、计费功能。

比如配置radius-server为192.168.0.111,通信密钥为“DSA4000”。

- DSA4000#radius auth ip 192.168.0.111 key DSA4000
- DSA4000#radius auth port 1812
- DSA4000#radius auth enable
- DSA4000#radius acct ip 192.168.0.111 key DSA4000
- DSA4000#radius acct port 1813
- DSA4000#radius acct enable

在和Radius Server配合时，要配置正确的认证、计费端口。旧的Radius协议定义的认证、计费端口为1645、1646，而新的Radius协议采用的认证、计费端口为1812、1813。

【注意】：DSA-4000/8000系列在2005年3月以后的IOS中Radius模块默认的认证、计费端口为1812，1813。在此之前的提供的IOS中，Radius 模块默认的认证、计费端口为1645，1646。

- DSA4000＃radius auth_switch_num 3

  设置当有3个用户认证不成功时，将用户认证从主Radius切换到备用Radius。同样当配置radius acct_switch_num 3时当有3个用户认证不成功时用户计费将从主Radius转换到备用Radius。

【注意】：D-LINK BRAS系列在2005年11月以前的IOS中主备切换的条件是一个用户认证不通过，不能配置切换条件。此后发布的版本可以根据用户需要进行切换条件设置，切换时间的设置可以根据radius timeout和radius retry进行计算。

- DSA4000＃radius mon_primary on

  打开主Radius工作状态监控开关，主要作用是当主Radius服务器工作异常时BRAS根据radius mon_interval <secondes>命令设置的时间间隔（默认30秒）定期检测主Radius服务器是否恢复正常工作。当配置一个Radius服务器时，BRAS也认为其是主Radius服务器。BRAS判断主Radius服务器恢复正常的依据是：BRAS发送的account-on报文得到主Radius 服务器的响应。

- DSA4000＃radius mon_down on

  DSA4000＃ radius mon_down_num 5

  这两个命令配置当BRAS发现没有一个Radius服务器能够正常工作时，有5个用户认证不能通过时就打开用户免认证开关（相当管理员手工设置set noauth on）。

  默认情况下该功能是关闭的。如果该功能打开，默认的切换条件是10个用户不能认证就自动打开免认证开关。当系统恢复正常认证时，免认证开关会自动关闭。

【注意】：DSA BRAS 关于Radius的默认参数配置如下：

radius mon_primary on

radius mon_interval 30

radius mon_down off

radius mon_down_num 10

radius auth_switch_num 1

radius acct_switch_num 1

网络管理员需要根据现场实际环境进行灵活设置。

4.27. reboot

【用法】：reboot

【作用】：重启机器。在改变某些敏感配置（例如端口地址或者端口属性）后或根据需要重新启动服务器。

【例如】：

- DSA4000# reboot

  重启机器。

4.28. route

【用法】：route add/del <net> <mask> <gateway>

route show

【作用】：修改、显示路由表。当在网络实际环境使用时，需要加入若干静态路由或者缺省路由到DSA-4000/8000中，使报文可以正确到达目的地址。

【例如】：

- DSA4000#route add 0.0.0.0 0.0.0.0 202.96.196.5

  增加缺省静态路由，所有报文都送到下一跳202.96.196.5。

- DSA4000#route show

  显示系统的路由表状况。

- DSA4000#route del 0.0.0.0 0.0.0.0 202.96.196.5

  删除缺省的静态路由。

4.29. set

【用法】：set nat_tcptimeout <sec>

set nat_udptimeout <sec>

set nat_icmptimeout <sec>

set chk_mac on/off

set user_telnet on/off

set md5_alive   on/off

set session_slow on/off

set nas_ip <ip>

set aaa_ext_attr on/off

set web_portal   on/off

set disable_winWeb on/off

set chk_pass on/off

set chk_pass_num <num>

set chk_cli_ip on/off

set long_uname on/off

set spec_logout on/off

set logout_ip <ip>

set noauth off

set pass_noip_stack on|off

set ctrl_nat_auth on|off

set pass_noip_stack on|off

set net_fast on| off

set net_poll on| off

set deny_bt on | off

set vendor_attr on | off

set cap_acl_flow on | off

【作用】：设置某些网络参数或者开启某些网络功能。

- set nat_tcptimeout <sec>

  设置 NAT 功能开启后的 tcp 连接的老化时间。

- set nat_udptimeout <sec>

  设置 NAT 功能开启后的 udp 报文的老化时间。

- set nat_icmptimeout <sec>

  设置 NAT 功能开启后的 icmp 报文的老化时间。

- set chk_mac on/off

设置是否使用MAC地址检查功能，开启后系统将对每个用户的MAC地址进行检查。该功能主要是为了防止用户异常掉线后，有人盗用该用户 IP 地址进行上网而设计的。

- set user_telnet on/off

设置是否允许本地用户进行 telnet 登录。

- set md5_alive   on/off

打开或者关闭 keepalive 报文的 MD5 加密功能。

- set session_slow on/off

打开或者关闭非时长用户使用的 Radius 协议中 session_slow 私有属性功能。

- set nas_ip <ip>

设置 nas_ip 地址，这个主要是和 Radius server 配合，给出 Radius Server 表示用户从哪个 NAS（Network Access Server）接入。

【注意】：NAS_IP 的设置需要根据 Radius Server 连接的 DSA-4000/8000 的端口 IP 进行设置：如果 Radius Server 和上行端口相联，则 set nas_ip 设置为上行端口的 IP 地址；同理，如果 Radius Server 和下行端口相联，则 set nas_ip 设置为下行端口的 IP 地址。因为该参数地址的设置，涉及到和 D-LINK DRS 系统中的用户管理模块中的服务器绑定功能，因此一定要根据网络实际情况正确设置。

- set Web_portal   on/off

打开或者关闭 Web_portal 功能。关闭 Web_portal 功能时，此时用户只能用专用客户端认证，不能使用 Web 认证。

- set disable_winweb on/off

是否关闭 windows 操作系统的 Web 认证功能。当为 set disable_winweb on 时，此时 Windows 用户不能使用 Web 认证。

当 set web_portal on，set disable_winweb on 时，此时只有 Linux 和 Mac 机可以使用 Web 认证，Windows 用户不能使用 Web 认证。

- set chk_pass on/off

打开 pass 用户检查开关，该命令和 set chk_pass_num 配合使用。

- set chk_pass_num <num>

设置 pass 用户的检查门限。当 set chk_pass on 时，如果 pass 用户的数量超过指定的门限时，系统对定期对 pass 用户状态进行检查，清除没有进行业务的 pass 用户的信息，释放这些 pass 用户占用的 BRAS 资源。这个功能主要是为了防止：当配置了太多的 pass

用户 ip 地址，有人假冒 pass 用户 ip 地址访问 Base，造成 BRAS 建立太多 pass 用户 session，消耗掉 BRAS 资源。

- set chk_cli_ip on/off

  对用户使用 SOHU router 认证上网进行控制.如果设置为 set chk_cli_ip on 不允许用户通过 SOHU route 进行上网，默认情况下为 set chk_cli_ip off。

- set long_uname on/off

  是否给 Radius Server 发送带有域名的用户名信息。一般情况下 BRAS 给 Radius Server 发送的用户名就是客户端或者 Web 认证时填写的用户名，不带有服务名，如 username。当设置 set long_uname on 时，BRAS 给 Radius Server 发送的用户名包括了服务名，如 username@DSA4000。**何种情况下启用该功能，必须要核实 Radius Server 是否支持该功能，否则可能导致用户不能正常认证。**

- set spec_logout on/off

  是否打开特殊退出方式，在 Web 认证时有时候因为 3721 等软件的拦截会导致连接小窗口被屏蔽，这时用户没有办法主动离线，为解决这个问题此时必须打开该功能。

- set logout_ip 1.1.1.1

  设置用户主动离线时在 IE 浏览器地址栏输入的地址，默认情况输入的地址是 http://1.1.1.1。该命令是配合set spec_logout on来使用的。

- set noauth on/off

  设置特殊情况下打开客户免认证功能，在极端情况下 Radius 服务器故障导致用户不能进行认证，此时可以打开该功能保证用户在任何用户名和密码下都能认证。**注意该命令平时应该处于 off 状态，只能在特殊情况下打开。在 Radius 机制中也设计有当所有 Radius Server 都没有响应时，自动打开免认证的机制，详见 radius 命令说明。**

- set pass_noip_stack on|off

  在**桥接模式下**是否对 STP 等协议进行透传设置，主要是为了在大型网络中满足用户高可靠性要求而设计。当配置 set pass_noip_stack on 时允许透传，否则不允许透传，默认情况下是 off。

- set aaa_ext_attr on/off

  是否打开 radius 扩展属性开关，该命令主要是为了和 Windows IAS 系统自带的 Radius Server 相配合而设计的。因为 Windows 系统自带的 Radius Server 不支持 Radius 协议的扩展属性，而通常情况下 D-LINK BRAS 系列产品都会用到 Radius 扩展属性，所以

系统默认情况下该命令是 on 的，只有和 Windows IAS 相配合才设置为 off。

- set ctrl_nat_auth on/off

  是否允许 nat 设备后用户进行认证。如果设置为 on，同时需要在 session 命令中增加 session address 254.254.0.0 的虚拟 session 设置，默认情况下是 off。该功能的使用主要是为了适应有些网络中用户在防火墙进行 NAT 变换而需要认证和计费的情况。

- set net_fast on/off，set net_poll on/off

  快速转发模式的打开或者关闭，该命令只是为了测试系统效率而设计，实际使用中必须处于 off 状态。

- set deny_bt on/off

  是否禁用 P2P 软件的使用，默认情况不禁用 P2P 软件。当设置 set deny_bt on 时，禁用 BT，eMule 的使用。由于 BT 等软件变种较多，因此该功能并不能完全禁用所有的 P2P 协议。

- set vendor_attr on/off

  是否将扩展属性封装到 Radius 26 属性中，默认情况下是不封装

- set cap_acl_flow on/off

  是否允许 BRAS 设备采集 ACL 流量，默认情况下 BRAS 设备不采集 ACL 规则的流量，而是由客户端软件进行 ACL 流量的采集和发送（**注意该功能必须是采用客户端进行认证情况下才能处于 on 的状态**）。ACL 功能的解释详见 ACL 命令的解释。

【例如】：

- DSA4000# set nat_tcptimeout 300

  设置 NAT 情况下，TCP 报文的老化时间为 300 秒。

- DSA4000#set user_telnet   on

  允许用户以 telnet 方式登录设备。

- DSA4000# set md5_alive off

  关闭 keepalive 报文的 MD5 加密功能。

- DSA4000# set session_slow on

  打开 Radius 协议的 slow_timeout 属性，该功能开启后 DSA-4000/8000 将对非时长用户（如流量用户或者包月用户）不检查 keeplive 报文的连接情况，此命令经常和 session idle_chk 命令一起使用。

- DSA4000#set nas_ip 192.168.0.2

设置 nas_ip 地址为 192.168.0.2，注意此时 Radius Server 和 DSA-4000/8000 的这个接口地址相连。

- DSA4000#set web_portal on

  DSA4000#set disable_winweb on

  关闭 windows 系统的 Web 认证功能,只允许 Linux 系统和 Mac 系统使用 Web 认证功能。

- DSA4000#set chk_pass on

  DSA4000#set chk_pass_num 1000

  当 pass 用户的数量达到 1000 时，系统开始定期检查 pass 用户的信息，释放没有进行业务的 pass 用户占用的资源。

【注意】：set chk_pass on 功能只有在系统存在大量 pass 用户时开启，并且 pass 用户检查的门限值不能太小，该功能默认情况下是关闭的。

- DSA4000＃set chk_cli_ip on

  禁止用户通过路由器作 NAT 进行认证上网。

- DSA4000＃set pass_noip_stack on

  在桥接模式下，允许 STP 报文进行透传。在桥接模式下，DSA-4000/8000 对 DNS、SNMP、RIP、OSPF、telnet 等协议是默认透传处理的，主要方便进行大型网络组网。

4.30. session

【用法】：

```
session address <begin_ip> <num> [pass|pass_out]- [inrate] [outrate]
session echo_timeout <second>
session echo_interval <second>
session slow_timeout <minute>
session acct_interval <minute>
session pass_in_rate <kbits/s>
session pass_out_rate <kbits/s>
session idle_chk enable/disable
session idle_timeout <minute>
session idle_data    <kbits>
```

session max_nat_num <num>

session web_num <num>

session msrv udp|tcp <port>

session no_msrv udp|tcp <port>

session osrv_rate <inRate> <outRate>

session limit_osrv enable|disable

session bt_rate <inRate> <outRate>

session limit_bt enable|disable

session clr_bpass

session limit_bt_tm <begin hh:mm> <end hh:mm>

session limit_bt_tm enable/disable

session limit_bt_tm show

【作用】：设置用户连接网络的参数。

- DSA4000#session address <begin_ip> <num> [pass|pass_out] [inrate] [outrate]

  设置允许接入网络的用户 IP 地址。如果有 pass 或者 pass_out 参数表示用户访问外网时无需认证；当配置 pass 或者 pass_out 时带有 inrate 和 outrate 表示对该 IP 子网的用户进行带宽限制。**该命令的优先级要高于 session pass_in_rate 和 session pass_out_rate 设置的参数**。

- DSA4000#session echo_timeout <second>

  设置页面连接窗口或者客户端软件和 DSA-4000/8000 多长时间没有 keepalive 报文交互，就切断其连接，默认时间为 180 秒。

- DSA4000#session slow_timeout <minute>

  设置非时长用户和 eFow BRAS 多长时间没有 keepalive 报文交互，就切断其连接，默认时间 300 分钟。

  该功能建议和 session idle_chk 命令配合使用，该命令要生效必须设置 set slow_timeout on。

- DSA4000#session echo_interval <second>

  设置 Web 认证的连接小窗口和 eFow BRAS 之间的 keepalive 报文的交互间隔时间，默

认时间 60 秒。

- DSA4000#session acct_interval <minute>

  设置 pass 用户计费报文的发送间隔，默认 60 分钟。如果用户不需要对 Pass 用户进行计费，可以将该参数设置为 0。

- DSA4000#session pass_in_rate <kbits/s>

  设置直通用户的上行速率。

- DSA4000#session pass_out_rate <kbits/s>

  设置直通用户的下行速率。

- DSA4000#session idle_chk enable/disable

  是否开启空闲检查功能。

- DSA4000#session idle_timeout <minute>

  设置空闲检查的时间间隔，默认 5 分钟。

- DSA4000#session idle_data <kbits>

  设置空闲检查的流量信息，默认 5kbits。

- DSA4000#session max_nat_num <num>

  设置用户默认情况下的 NAT 会话量，默认 300 条。

- DSA4000#session web_num <num>

  设置每个用户最多可以发起的 Web 认证的连接数，默认 10 个。为防止针对 DSA-4000/8000 内置 Web Server 的 DOS 攻击，建议一般情况将该参数设置为 5 个。

- DSA4000# session limit_osrv enable|disable

  是否打开根据应用层业务进行带宽控制的开关，默认是关闭该功能的，即该命令是 disable 状态。D-Link 根据应用层进行带宽控制的机制是定义若干常用业务,如 web，邮件，ftp 等为主流业务，该主流业务以外的上层应用为非主流应用，可以通过命令来在用户总带宽中分配部分带宽用于非主流业务。这个是 D-LinkDSA-4000/8000 进行 P2P 软件应用的机制之一。

- DSA4000＃session msrv udp|tcp <port>

  定义主流业务的使用的协议（udp,tcp）和 port 号。

- DSA4000＃session no_msrv udp|tcp <port>

  取消定义的非主流业务的定义。

- DSA4000＃session osrv_rate <inRate> <outRate>

定义非主流业务的上行带宽和下行带宽。

- DSA4000＃session limit_bt enable|disable

  是否单独对 P2P 软件进行带宽控制。

- DSA4000# session bt_rate <inRate> <outRate>

  设置 P2P 软件的可以使用的上行和下行带宽。

- DSA4000＃session clr_bpass

  将已经停用的 pass 用户状态恢复为可用，该命令是防止 D-LINK DRS 系统和 DSA-4000/8000 系统改变 pass 用户状态失效的情况的一个补充手段，一般只有 DRS 系统命令失败情况才使用。

- DSA4000＃session limit_bt enable|disable

  根据时间控制 p2p 带宽参数是否打开，默认是关闭的。

- DSA4000＃session limit_bt_tm <begin hh:mm> <end hh:mm>

  设置带宽控制的起始时间、结束时间，以 24 小时制为准

- DSA4000＃session limit_bt_tm show

  查看根据时间控制 P2P 软件是否生效，allow 为 1 是生效，为 0 失效。

【注意】：**默认情况下，如果不打开 session limit_bt enable 开关，那么对于 P2P 软件的带宽控制是在任何时候都可以起作用（前提为配置了** session limit_bt enable 和 session bt_rate <inRate> <outRate>命令情况下)，**但配置了该功能后，只有在规定的时间内对 P2P 软件的带宽控制才生效。**

【例如】：

- DSA4000#session address 10.1.1.2 250

  允许用户使用 10.1.1.2 开始的 250 个 IP 地址进行接入。

- DSA4000#session address 10.1.1.220 10 pass

  允许用户使用 10.1.1.220 开始的 10 个 IP 地址无需认证，当这些用户从接入端口访问外网时无需认证，但是外网用户不能主动访
问 10.1.1.220 开始的 10 个 IP 地址。

- DSA4000#session address 10.1.1.220 10 pass 256 512

  设置 10.1.1.220 开始的 10 个地址为 pass 用户，这些用户的上行速率为 256kbps，下线速率为 512kbps。

- DSA4000# session address 10.1.1.220 10 pass_out

允许用户使用10.1.1.220开始的10个IP地址无需认证，当这些用户从接入端口访问外网时无需认证，同时外网用户也可以主动访问10.1.1.220开始的10个IP地址。这种配置主要用于对外提供服务的WEB、FTP、Telnet等服务器的设置，方便用户从公网访问。

【注意】：

因为 session 命令中 session echo_interval/echo_timeout，session idle_chk，session slow_time 这3组命令都涉及到DSA-4000/8000和用户端（Web认证或者client认证）之间的keepalive报文的交互，影响DSA-4000/8000判断用户异常下线的条件，所以有必要对这3组参数之间的关系进行深入的讲解。

D、 session echo_interval/echo_timeout：

当使用 Web 认证时，用户端和 BRAS 之间 keepalive 报文的发送间隔是 session echo_interval 决定的，当BRAS在session echo_timeout时间内没有收到keepalive报文，就会判断用户异常，从而停止用户计费。

当使用专用客户端进行认证时，session echo_interval 对客户端没有作用，但是如果当BRAS在session echo_timeout时间内没有收到keepalive报文，就会判断客户端异常，从而停止用户计费。因为此时客户端软件同时会判断BRAS异常，如果客户端在150－200秒内没有收到BRAS响应的keepalive报文，就会自动掉线。

E、 session idle_chk enable、session idle_timeout、session idle_data：

当打开session idle_chk enable功能时，系统将会对每个用户的流量信息检查。如果在session idle_timeout时间内用户的流量没有达到session idle_data指定的流量门限，则系统会强制用户下线。

Session idle_chk 功能打开后，如果用户满足 session echo_interval,session echo_timeout或者session idle_timeout,session idle_data这两组条件之一就会被强制下线。**2006年5月以后V2.9版本的IOS修改了该机制，如果检查keepalive异常，还会检查idle_chk相关参数进行判断，只有两个条件同时满足才会将用户session删除。**

F、 session slow_timeout：

当设置 set slow_timeout on时，对非时长用户将不再检查keepalive报文（不管是使用Web认证还是专用客户端认证）。非时长用户上网时间到达session slow_timeout设置的值后：如果没有打开 session idle_chk 功能，该用户将自动掉线；如果打开 session idle_chk功能，系统将根据该session idle_chk设置的参数进行流量检查，此时判断用户

异常的条件是在指定的时间内没有到达指定的流量值。

这三组参数之间的关系比较复杂，请大家一定要认真理解它们之间的相互关系，这样才能根据网络情况灵活的进行设置相关参数。

- DSA4000# session msrv tcp 110 （email smtp）

  DSA4000#session msrv tcp 21   （FTP）

  DSA4000#session msrv tcp 20   （FTP）

  DSA4000#session msrv tcp 23   (Telnet)

  DSA4000#session msrv tcp 25   （mail POP3）

  DSA4000#session msrv tcp 80   （web）

  DSA4000#session osrv_rate 64 64

  定义除上述定义以外的非主流业务的上行带宽和下行带宽为 64kpbs。

  DSA4000#session limit_osrv enable

  打开根据业务类似进行带宽控制的开关。

- DSA4000# session bt_rate 128 128

  DSA4000#session limit_bt enable

  设置 P2P 软件使用的上行带宽和下行带宽为 128kbps

【注意】**上述两种对 P2P 软件的控制方法，可以同时分别起作用。建议：在实际应用中只能使用其中一种机制进行控制。**

- DSA4000#session limit_bt_tm enable

  对 P2P 软件使用的带宽根据时间进行控制

- DSA4000# session limit_bt_tm 19:00 23:00

  每天 19:00 到 23:00 对 P2P 软件使用的带宽根据时间进行控制，其它时间不予以控制。

- DSA4000# session limit_bt_tm show

  System Start Time: MON MAY 29 19:34:34 2006 BRAS 系统启动时间

  System Run   Time: WED MAY 31 20:20:47 2006 当前 BRAS 的系统时间

  Limit BT rate allow: 1 1   当前根据时间控制 P2P 软件带宽是生效的

  session limit_bt_tm 19:00 23:00 19:00 到 23:00 对 P2P 软件带宽进行控制

  session limit_bt_tm enable

4.31. servicename

【用法】：servicename <name> [pri_dns] [sec_dns]

【作用】：定义服务的名称，其中[pri_dns] [sec_dns]为可选项，适用于服务和DNS server绑定的场合。如果采用Radius认证计费，则应该和Radius服务策略中定义的服务类型结合起来。

【例如】：

- DSA4000# servicename local

  定义服务的名称为local

- DSA4000# servicename internet

  定义服务的名称为internet

【注意】：旧的版本，show servicename 同 write 配置次序不同。2006年5月V2.9版本修改了相关问题，可以按正常配置顺序进行显示。

【参考命令】：aclcfg。

4.32. show

【用法】：show <var>

【作用】：显示系统的各种参数，该命令最为常用。

【例如】：

- DSA4000＃show ？

  列出可以显示的各种系统参数。

- DSA4000＃ show config

  显示已配置参数。

- DSA4000＃show bridge

  显示桥接工作模式下的收发包情况。

- DSA4000＃

- DSA4000# show ?

```
show config              -- show all configuration
show aaa                 -- show radius client info
show acl  [num]          -- show acl-tree configuration
```

```
show aclcfg            -- show acl's access on/off
show arp               -- show arp table
show arpBind           -- show ip & mac Binding info
show auth              -- show authentication type
show back_rt           -- show back_rt cfg
show back_rt_info      -- show back_rt info
show bt_ses            -- show limit bt rate info
show  cli_info         -- show client dbg info
show  ctrl_bpass       -- show block pass ses
show  ctrl_cfg         -- show block pass ses config
show dhcp              -- show dhcp configuration
show deny_bt           -- show deny_bt info
show ha                -- show ha configuration
show ha_info           -- show ha running info
show hostname          -- show hostname configuration
show icmpin            -- show icmp controlling status
show icmpstat          -- show icmp statistics
show ipstat            -- show ip statistics
show enet0/1/2/3       -- show port status
show link [name]       -- show link level informations
show logger            -- show log configuration
show man_info          -- show man interface
show memory            -- show memory
show nameserver        -- show nameserver configuration
show netstat           -- show network connections
show net_fast          -- show net fast path
show pnp               -- show plug and play configuration
show pool              -- show pool configuration
show port              -- show port configuration
show proxyarp          -- show proxyarp table
```

```
show psgw               -- show connect pseudo gateway
show radius             -- show radius configuration
show route              -- show route table
show tcplimit           -- show tcp concurrent link number
show tcpstat            -- show tcp statistics
show servicename        -- show servicename configuration
show set                -- show system set
show session  [ip]      -- show  sessions
show session_num        -- show  sessions num
show session_pass       -- show  pass sessions detail
show session_cfg        -- show session configuration
show snmp               -- show snmp community
show syn_ses            -- show syn session cfg
show syn_ses_info       -- show syn session info
show system             -- show system information
show udpstat            -- show udp statistics
show version            -- show system verion
show webp               -- show web portal configuration
show ?                  -- show help
```

4.33. snmp

【用法】：snmp com name r|w|rw

snmp trap <ip>

snmp trap_version <num>

【作用】：配置 snmp 协议 community 及读写权限，trap 报文发送的地址和报文的版本号。

【例如】：

- DSA4000＃snmp com DSA4000 r

  设置设备 snmp 协议的 community 参数为 DSA4000，只有读的权限。

- DSA4000＃snmp com admin rw

设置设备 snmp 协议的 community 参数为 DSA4000，具有读写的权限。

- snmp trap 192.168.0.100

  将 snmp 相关信息发送到管理主机 192.168.0.100。

- snmp trap_version 1

  snmp trap 报文按 snmp v1 定义的格式发送。

4.34. src_route

【用法】：src_route enable/disable　使能/禁止源地址路由

src_route show 查看源地址路由

src_route add/del <net> <mask> <next_hop>

【作用】：配置源地址路由功能，增加或者删除一条源地址路由配置。增加以后，只要 ip 包的源 ip 落在给定的网络地址掩码范围内，那么不论其它路由配置如何，都把该 ip 包转发给指定的下一跳地址的网关。

【例如】：

- DSA4000# src_route enable
- DSA4000# src_route add 10.1.2.0 255.255.255.0 192.168.0.3
- DSA4000# route add 0.0.0.0 0.0.0.0 192.168.0.2

该命令假设设备上行口 192.168.0.1,有两个上行出口分别是:192.168.0.2 和 192.168.0.3。用户地址段为 10.1.1.0/24 和 10.1.2.0/24，默认路由是 192.168.0.2，而 10.1.2.0 地址段的用户走 192.168.0.3 的路由。

【参考命令】：route

4.35. syn_session

【用法】：syn_ses　server <ip>

syn_ses　key <key>

syn_ses　timeout <second>

syn_ses　mode　srv|cli|ha

syn_ses　enable|disable

【作用】：对两台 DSA-4000/8000 的 session 进行同步控制，主要是组网中为了提高网络可

靠性时采用两台 DSA-4000/8000 进行双机热备组网或者多出口时用户进行一次认证即可进行网络访问而设计。详细的配置应用见附件常见问题的说明。

- DSA4000#syn_ses server <ip>

  配置需要进行同步 session 的 BRAS 的 IP 地址。

- DSA4000# syn_ses key <key>

  配置需要同步 session 的两台 BRAS 之间通信密钥。

- DSA4000＃syn_ses timeout <second>

  配置需要同步 session 的两台 BRAS 之间通信的超时时间。

- DSA4000# syn_ses mode srv|cli|ha

  配置 session 同步的工作模式，服务器、客户端模式还是 HA 情况下同步。

【注意】：如果设备配置了 HA Enable， 需要配置模式为 HA.

- DSA4000＃syn_ses enable/disable

  session 同步功能打开或者关闭。

【例如】：

- DSA4000# syn_ses key DSA4000

  配置需要同步 session 的两台 BRAS 之间通信密钥为 DSA4000。

- DSA4000# syn_ses mode ha

  配置两台 BRAS 直接 session 同步的模式为 ha。

- DSA4000#syn_ses enable

  打开 session 同步功能。

4.36. tcplimit

【用法】： tcplimit disable/enable/show

tcplimit default [num1] [num2]

tcplimit user [ip]

tcplimit pass_user enable/disable

【作用】： 对用户的 TCP 连接会话数进行限制，查看用户当前的会话数。

【例如】：

- DSA4000#tcplimit enable

打开 TCP 会话限制功能。

- DSA4000#tcplimit default 30

  设置用户默认的所有 TCP 会话连接数为 30。

- DSA4000#tcplimit default 30 30

  设置用户默认的非 tcp 80 会话连接数为 30，tcp 80 会话连接数为 30，这种配置的目的是保证 tcp 80 优先于其它 tcp 连接。

- DSA4000#tcplimit user 192.168.0.189

  查看 192.168.0.189 当前的会话数。

- DSA4000#tcplimit pass_user disable

  对 pass 用户（包括 pass_out）用户建立的 tcp 连接数不进行限制。Tcplimit enable 时，默认情况下 tcplimt pass_user 是 enable 的。

【注意】：tcplimit user [ip]命令显示的不一定是当前该用户的真实 tcp 连接，因为系统设计时为了减小 cpu 负荷，当用户的 tcp 连接数到达默认的极限时，用户新建的 tcp 连接就会替换原先的处于关闭状态的 tcp 连接。因此当用户实际 tcp 连接数大于或者等于设置的门限值后，tcplimit user [ip]命令看到的不一定是此时用户真实的 tcp 连接状况。

DSA-4000/8000 1103D 默认的最大 tcp 连接数可以设置为 30，
DSA-4000/8000 默认的最大 tcp 连接数可以设置为 100。

当用户打开该功能后，此时用户如果在 Radius Server 设置了该用户可以建立的 TCP 连接数，那么该用户认证通过后 Radius Server 返回的参数优先于 DSA-4000/8000 设置的 TCP 连接数。当你配置了 tcplimit defautlt num1 num2 时，Radius Server 设置的 TCP 连接数将优先于 num1,而该用户的 TCP 80 业务的连接数将限制为 num2。

特别是如果 Radius Server 设置了该用户可以建立的 TCP 连接数为空或者 0 时，表示对该用户建立的 TCP 连接数将不予限制（不管 BRAS 是否设置了 tcplimit default num1 num2），而此时 tcplimit user ip 将不显示该用户建立的 tcp 连接情况。

本地认证用户的 tcp 连接数按 BRAS 设置的 tcplimit default num1 num2 来进行控制。

4.37. telnet

【用法】：telnet ip [port]

【作用】：远程登录指定的主机，可以指定端口。

【用法】：

- DSA4000#telnet 192.168.0.189

  通过 telnet 登录 192.168.0.189 的设备。

4.38. telnetlist

【用法】：telnetlist add/del <ip> <mask>

telnetlist show

【作用】：添加或者删除指定的 ip 子网的主机可以登录 DSA-4000/8000，其他用户不能登录。

【用法】：

- DSA4000#telnetlist add 192.168.0.189 255.255.255.255

  允许主机 192.168.0.189 可以 telnet 登录本设备。

- DSA4000# telnetlist add 192.168.0.0 255.255.255.0

  允许子网 192.168.0.0 的用户 telnet 登录本设备。

【注意】：该命令目前只支持标准掩码，不支持可变长掩码（VLSM)。

4.39. time

【用法】：time [YYYYMMDDHHMM]

【作用】：显示和修改系统时间。

【例如】：

- DSA4000#time

  显示系统时间。

- DSA4000# time 200012031200

  设置系统时间为2000年12月03日12时 00分。

4.40. upgrade

【用法】：upgrade tftp_server file_name

【作用】：通过tftp server 升级系统。

【例如】：

- DSA4000# upgrade 202.96.196.3 ios

  到ip 地址为202.96.196.3 的 tftp server, 下载文件名为ios文件作为系统新版本。

【参考命令】:reboot

4.41. user

【用法】：user name <name> passwd <passwd>

【作用】：增加本地用户，用于本地认证或者telnet登录。

【例如】:

- DSA4000#user name admin passwd pass

  增加一个名字为admin密码为pass 的本地用户。

【参考命令】local

4.42. web

【用法】: web put|get tftp_server filename

web ls

web pr filename

web rm filename

【作用】: 配置、显示、删除相关 Web 认证的文件。要非常谨慎的使用该命令，使用前请和 D-Link 公司的技术支持人员联系。替换掉网页文件后，要执行 Webp recache 命令使新的文件生效。

【例如】:

- DSA4000#web get 192.168.0.189 cauth.asp

  从 TFTP Server 192,168.0.189 下载 cauth.asp 文件。

- DSA4000＃web ls

  显示所有与页面相关的文件。

- DSA4000＃web pr cauth.asp

  显示 cauth.asp 文件的内容。

- DSA4000＃web rm cauth.asp

  删除 cauth.asp 文件。

【参考命令】：webp

4.43. webp

【用法】：webp url <address>

webp pass <ip> <mask>

webp nopass <ip> <mask>

webp vlan_page enable/disable

webp vlan <vlan_id> <num> <portal_file>

webp del vlan <vlan_id> <num>

webp recache

【作用】：设置与 web portal 相关的功能。

- webp url <address>

  指定 Web portal，用户认证通过后强制登录指定 url。

- webp pass <ip> <mask>

  指定 IP 可以不用认证进行登录，此时用户访问该 IP 也不会限速和计费。

- webp nopass <ip>

  删除设定的免认证登录 IP。

- webp vlan_page enable/disable

  开启或者关闭 vlan 认证功能。

- webp vlan <vlan_id> <num> <portal_file>

  设置指定 vlan 认证的认证页面文件。

- webp del vlan <vlan_id> <num>

  删除指定 vlan 认证的 vlan ID。

- webp recache

  使上传的页面文件生效。

【例如】：

- DSA4000＃webp url http://www.dlink.com.cn

  用户认证后强制登录 www. dlink.com.cn。

- DSA4000＃webp url http://0.0.0.0

取消强制登录指定的 url。

- DSA4000＃webp pass 210.10.10.80 255.255.255.255

  访问 210.10.10.80 可以不用认证、不用计费、不用限速。

- DSA4000＃webp vlan_page 110 10 cauth.asp

  vlan 110-119 使用 cauth.asp 认证页面进行登录。

- DSA4000＃webp del vlan 110 10

  取消 vlan 110 到 vlan 119 的 vlan 认证功能。

4.44. write

【用法】：write

【作用】：存储配置参数到flash memory 中。

【例如】:

- DSA4000# write

  将当前配置文件存储到flash memory。

5. 常见问题

5.1. 如何登录主机?

从串口连入主机, 以用户名 admin 密码 dlink 登录主机。

telnet 登录主机, 必须是以机器设置的本地认证用户登录,且设置 set user_telnet on 允许用户远程登录。

5.2. 如何进行初始配置?

具体情况可以参见本手册第三章。

一般来说，登录进入服务器以后，最开始的配置是对端口的配置（参见port命令详解）。在进行这个配置后，先用write把配置保存起来，然后重新启动机器(reboot)使配置生效;

然后，重新登录进去，这时系统最基本配置已经生效，根据情况可以配置如下：

- 路由配置（参见 route 命令详解）;
- Radius 以及本地认证配置（参见 radius、auth、local 等命令详解）;
- 本地用户配置（参见 user 命令详解）;
- NAT 配置（参见 NAT 命令详解）;
- 主机名配置（参见 hostname 命令详解）;
- 服务配置（参见 servicename 命令详解）;
- 域名服务器配置（参见 nameserver 命令详解）;

在配置完成后，可以用write命令把所有命令保存起来。

还有一种方式可以进行配置。用cfg命令从tftp服务器上把适合自己的配置文件download下来，然后reboot既可。

5.3. 如何取得配置权限?

从串口连入主机, 键入 enable,默认的密码为 dlink。

telnet 登录主机, 必须是设置的enable 密码。

建议：配置好文件后修改默认的enable密码，以保证安全。

5.4. 如何配置端口？

假设端口0使用以太网协议，ip地址为202.96.196.1 掩码为 255.255.255.0；设置系统最多可连接200个认证用户。

配置方法：

DSA4000#port enet0 ethernet 202.96.196.1 255.255.255.0

DSA4000#session address 202.96.196.2 200

5.5. 如何配置 Radius?

假设Radius服务器IP地址为172.18.86.189，key为“DSA4000”，认证和记费功能均为打开。

配置方法：

- DSA4000#radius auth ip 172.18.86.189 key DSA4000
- DSA4000#radius auth enable
- DSA4000#radius acct ip 172.18.86.189 key DSA4000
- DSA4000#radius acct enable

【注意】：认证和计费端口的配置根据Radius系统实际使用的端口进行配置。老的Radius标准使用的认证、计费端口是1645、1646，新的Radius认证、计费端口是1812，1813。DSA-4000/8000系列产品在2005年3月以前的IOS中，默认的认证、计费端口是1645、1646；在此之后的IOS默认使用的认证、计费端口采用1812、1813。

5.6. 如何配置 filist?

filist主要针对过滤规则进行设置，可以对地址和端口进行特定的过滤，控制用户对网络的访问。

假设用户的地址在10.1.1.0 ～ 10.1.1.255网段，通过端口enet1拨入，需要过滤掉所有用户的icmp数据。

设置如下：

DSA4000#filist add enet1 block in icmp 10.1.1.0/24 0.0.0.0/0

如果要阻塞所有的包，则现在暂时不能使用ip协议，需要三条规则分别针对tcp,udp,icmp协议。假设需要阻塞所有从地址10.1.1.0 ～ 10.1.1.255到地址192.168.1.2的数据，设置如下：

- DSA4000#filist add enet1 block out tcp 10.1.1.0/24 192.168.1.2/32 quick
- DSA4000#filist add enet1 block out udp 10.1.1.0/24 192.168.1.2/32 quick
- DSA4000#filist add enet1 block out icmp 10.1.1.0/24 192.168.1.2/32 quick

5.6.1. 利用 filist 设置拨号上来的用户互相不能通信

假设有一个接入端口(enet1)10.1.1.0 ～ 10.1.1.255，要让拨号上来的用户互相不能通信，只能访问外面，配置如下：

- DSA4000#filist add enet1 block in tcp 10.1.1.0/24 10.1.1.0/24 quick
- DSA4000#filsit add enet1 block in udp 10.1.1.0/24 10.1.1.0/24 quick
- DSA4000#filist add enet1 block in icmp 10.1.1.0/24 10.1.1.0/24 quick

5.6.2. 利用 filist 限制访问国外站点

假设enet1（10.1.1.0 ～ 10.1.1.255）的用户不允许访问国外站点，（设国内的站点是以61或210、202开始的地址，DNS假设为202.96.128.68），enet0为上行端口。配置如下：

- DSA4000#filist add enet0 pass out tcp 10.1.1.0/24 61.0.0.0/8 quick
- DSA4000#filist add enet0 pass out udp 10.1.1.0/24 61.0.0.0/8 quick
- DSA4000#filist add enet0 pass out icmp 10.1.1.0/24 61.0.0.0/8 quick
- DSA4000#filist add enet0 pass out tcp 10.1.1.0/24 202.0.0.0/8 quick
- DSA4000#filist add enet0 pass out udp 10.1.1.0/24 202.0.0.0/8 quick
- DSA4000#filist add enet0 pass out icmp 10.1.1.0/24 202.0.0.0/8 quick
- DSA4000#filist add enet0 pass out tcp 10.1.1.0/24 210.0.0.0/8 quick
- DSA4000#filist add enet0 pass out udp 10.1.1.0/24 210.0.0.0/8 quick
- DSA4000#filist add enet0 pass out icmp 10.1.1.0/24 210.0.0.0/8 quick
- DSA4000#filist add enet0 block out tcp 10.1.1.0/24 0.0.0.0/0 quick
- DSA4000#filist add enet0 block out udp 10.1.1.0/24 0.0.0.0/0 quick
- DSA4000#filist add enet0 block out icmp 10.1.1.0/24 0.0.0.0/0 quick

5.7. 如何配置 nat ？

nat有几种规则：第一种是把一段地址映射到一段地址，只是地址改变，通讯端口保持

不变。第二种是把一段地址映射到一个地址，所有的内部地址使用同一个出口地址，在此地址上进行端口映射。第三种是前面两种的结合，把一个地址映射到另外一个地址，或者针对端口进行转换。

假设端口0为上行端口并且使用以太网协议，ip地址为202.96.196.3掩码为255.255.255.128。内部用户使用地址为 10.1.1.0 到10.1.1.255，进行第二种转换。

配置方法：

- DSA4000#port enet0 ethernet 202.96.196.3 255.255.255.128
- DSA4000#session address 10.1.1.1 256
- DSA4000#nat add map enet0 10.1.1.0/24 202.96.196.3/32 portmap
- DSA4000#nat add map enet0 10.1.1.0/24 202.96.196.3/32

假设分配一个专用的地址给用户，用户的内部地址为10.1.1.2，给他分配一个固定的外部地址192.168.1.1。

配置如下：

- DSA4000#nat add map enet0 10.1.1.2/32 192.168.1.1/32
- DSA4000#nat add rdr enet0 192.168.1.1/32 10.1.1.2/32

假设要把所有访问192.168.1.89的数据重新定向到10.1.1.1上，可以配置如下：

- DSA4000#nat add rdr enet0 192.168.1.89/32 10.1.1.1/32

6. Radius 属性支持

6.1. Radius 属性表：

属性名	属性值	描述
PW_USER_NAME	1	用户名
PW_PASSWORD	2	密码
PW_CHAP_PASSWORD	3	
PW_NAS_IP	4	
PW_NAS_PORT	5	
PW_SERVICE_TYPE	6	
PW_FRAMED_PROTOCOL	7	
PW_FRAMED_ADDRESS	8	
PW_FRAMED_NETMASK	9	
PW_FRAMED_ROUTING	10	
PW_FRAMED_FILTER_ID	11	
PW_FRAMED_MTU	12	
PW_FRAMED_COMPRESSION	13	
PW_LOGIN_HOST	14	
PW_LOGIN_SERVICE	15	
PW_LOGIN_TCP_PORT	16	
PW_OLD_PASSWORD	17	
PW_PORT_MESSAGE	18	
PW_DIALBACK_NO	19	
PW_DIALBACK_NAME	20	
PW_EXPIRATION	21	
PW_FRAMED_ROUTE	22	
PW_FRAMED_IPXNET	23	
PW_STATE	24	
PW_SESSION_TIMEOUT	27	
PW_CALLED_STATION_ID	30	
PW_CALLING_STATION_ID	31	
PW_ACCT_STATUS_TYPE	40	
PW_ACCT_DELAY_TIME	41	
PW_ACCT_INPUT_OCTETS	42	
PW_ACCT_OUTPUT_OCTETS	43	
PW_ACCT_SESSION_ID	44	
PW_ACCT_AUTHENTIC	45	
PW_ACCT_SESSION_TIME	46	
PW_ACCT_INPUT_PACKETS	47	
PW_ACCT_OUTPUT_PACKETS	48	

PW_ACCT_DOWN_CAUSE	49	
PW_MAX_UPRATE	197	上行带宽
PW_MAX_DOWNRATE	198	下行带宽
PW_VLAN-ID	199	用户所在vlan
PW_Service-Name	200	提供的servicename
PW_Tcp-Limit	202	Tcp连接数限制
PW_Check_Cyc	203	Slow_time功能
PW_Amt-Version	204	客户端版本控制
PW_Amt-HttpUrl	205	客户端升级URL

6.2. 与 DSA-4000/8000 相关属性：

在BRAS接入服务器中除了常用的属性外,用到了Radius的几个私有属性,需要进行支持。

■ 最大上行速率：

在Radius端可以针对不同类型的服务，限制最大的上行速率，通过DSA-4000/8000接入服务器来实现。相应的Radius属性名为PW_MAX_UP_RATE。

■ 最大下行速率：

在Radius端可以针对不同类型的服务，限制最大的下行速率，通过BRAS接入服务器来实现。相应的Radius属性名为PW_MAX_DOWN_RATE。

■ 服务名称：

对应于所定义的服务类型。相应的Radius属性名为PW_SVR_NAME。

■ Tcp 连接数限制:

用于控制用户建立的TCP连接数，相应的Radius属性名为PW_Tcp_Limit。

■ 用户 VLAN_ID:

提供用户所在的VLAN_ID信息，从而进行用户名、密码和VLAN进行绑定，对应的Radius属性名为PW_VLAN_ID。

技术支持

办公地址：北京市朝阳区建国路 71 号惠通时代广场 C1 座 202 室 邮编: 100025

技术支持中心电话：8008868192/(028)85176977

技术支持中心传真：(028)85176948

维修中心地址：北京市朝阳区建国路 71 号惠通时代广场 C1 座 202 室 邮编: 100025

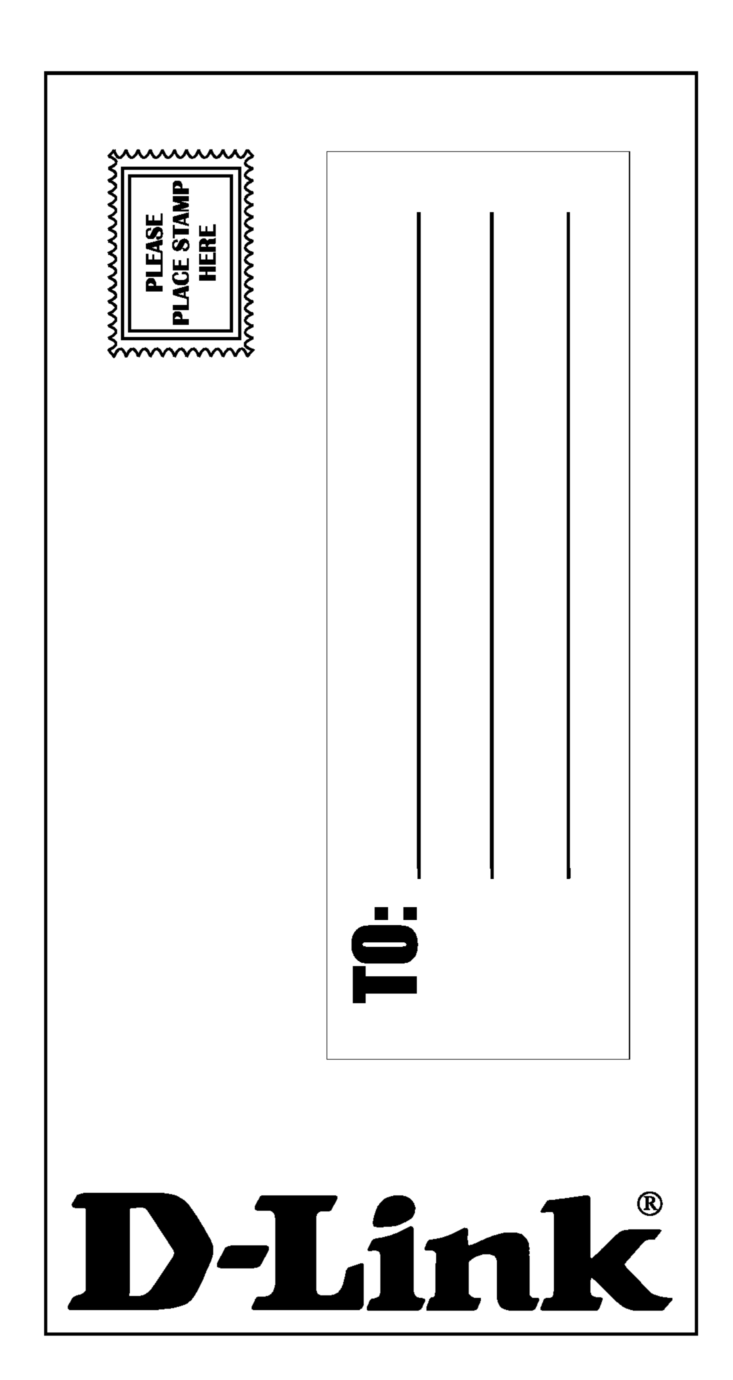
维修中心电话：(010) 58635800

维修中心传真：(010) 58635799

网址：http://www.dlink.com.cn

办公时间：周一到周五，早09:00到晚18:00




PLEASE
PLACE STAMP
HERE
TO:
D-Link®